Australian Government
Australian Digital Health Agency

National Secure Messaging Network Interoperability Specification

27 June 2023 v1.0

Approved for external use

Document ID: **DH-3569:2023**

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

National Secure Messaging Network – Interoperability Specification

Key information

Owner	National Chief Information Officer
Contact for enquiries	Australian Digital Health Agency Help Centre Phone 1300 901 001 Email help@digitalhealth.gov.au

Product or document version history

Product or document version	Date	Release comments
1.0	27 June 2023	Initial version

Table of contents

1. Introduction

1.1. Purpose

In recent years, Australian Digital Health Agency (ADHA) and its healthcare industry partners have been progressing towards the development of a National Secure Messaging Network (NSMN) that will enable reliable, secure electronic communication between Australian healthcare providers.

The NSMN Blueprint outlines the NSMN solution and defines the NSMN roles.

The NSMN Interoperability Specification (IS) details the technical requirements that underpin the NSMN.

The Interoperability Specification Requirements are structured around the Blueprint solution roles. The NSMN Solution Requirements define the requirements that each solution role must meet, and any solution constraints that must be adhered to when meeting those requirements.

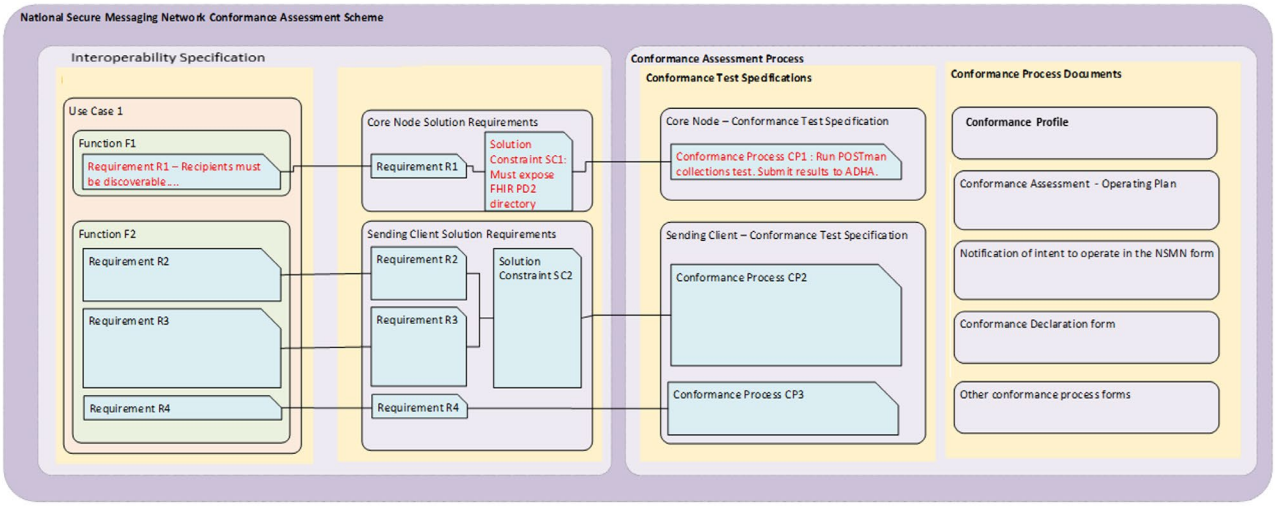

Figure 1 – The Interoperability Specification and the NSMN Conformance Assessment Scheme

In addition to this Interoperability Specification, the Conformance Assessment Scheme defines a set of Conformance Test Specification (CTS) documents that will guide the developer in understanding the complete conformance landscape for Secure Messaging.

As shown in Figure 1, these are “companion documents” to the Interoperability Specification. They define sets of tests that can be used to demonstrate conformance with the NSMN Conformance Profile.

1.2. Intended audience

This document is intended for organisations that intend to provide solutions that will participate in the NSMN. It is primarily intended for Business Analysts, Architects, Software Developers, Testers, and other technical staff involved in solution development.

1.3. Future considerations

1.3.1. Non healthcare providers

Currently, as per Appendix B, the only approved Certificate Authority (CA) for this version of the Interoperability Specification is NASH. The NSMN Interoperability Specification would need to be revised to support secure messaging communication with non-healthcare providers and entities that cannot obtain a NASH certificate.

1.3.2. Consumer messaging

Support for provider to consumer (patient) messaging is currently not in scope for this NSMN Interoperability Specification as the framework and use cases for this communication have not been defined. The NSMN Interoperability Specification would need to be revised to support secure messaging communication with consumers.

2. NSMN Interoperability Requirements

2.1. NSMN Interoperability Requirements

This section contains the NSMN Interoperability Requirements. The purpose of the Interoperability Requirements is described in section 1.1.

2.2. Structure of the Interoperability Requirements

The Interoperability Requirements list the use cases, functions, and software requirements that make up the formal requirements of the NSMN. The use cases are organised around "business actors" (e.g., Author, Intended Recipient, etc) and their business goals (e.g., Send a referral, Reconcile Messages, etc). These terms are defined in the NSMN Glossary at the end of this document.

Each use case consists of one or more functions that solutions must support when enabling that use case. Each function is in turn composed of one or more low-level requirements that are associated with the function. The Interoperability Requirements and its hierarchical structure are illustrated in Figure 2.

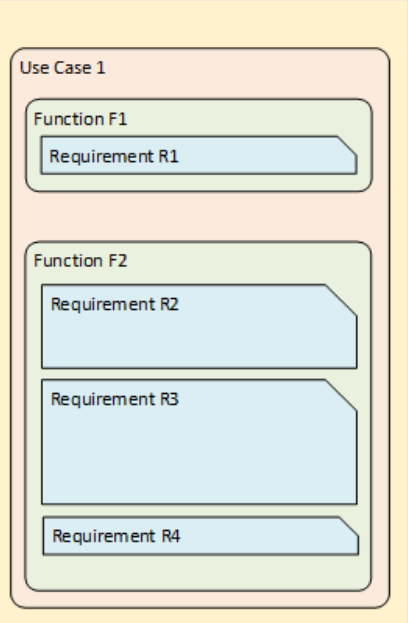

Figure 2 – Structure of Interoperability Requirements

The Interoperability Requirements are intended to be "solution neutral" – multiple solutions may be created that will meet the specified requirements.

2.3. Use Cases

The NSMN will support the following use cases.

2.3.1. UC1 Send referral

Description	During a consultation, the Author refers the Consumer to a Healthcare Service or Practitioner Role, the Intended Recipient.
Use Case #	UC1
Goal	To deliver a Referral for the Consumer to the Healthcare Service or Practitioner Role.
Primary Actor	Author
Other Actors	Consumer Sending System Provider Directory
Assumptions	The referral is sent during a consultation or soon after. The Sending System has a local record for the Consumer and has that record open during the consultation. The Consumer consents to be referred.
Pre-conditions	None
Triggers	With Consumer consent, the Author decides to refer the Consumer to the Healthcare Service or Practitioner Role.
Post-conditions	A referral is delivered to the Healthcare Service or Practitioner Role.

Basic flow of events

1. In consultation with the Consumer, the Author searches for and chooses a Healthcare Service or Practitioner Role to refer the Consumer to:
    a. The Author searches an online Provider Directory for the Intended Recipient- a Healthcare Service or Practitioner Role.
    b. The Author selects the Intended Recipient from the search results.
    c. The Sending System adds the Intended Recipient's name and identifier to the distribution list.
    d. The Author may repeat the process to add additional Healthcare Services or Practitioner Roles that the referral will be delivered to.
2. The Author opens the correct referral template in the Sending System for the selected Intended Recipient.
    a. The Sending System checks whether the Intended Recipient supports the chosen payload format.
3. The Sending System populates available information from the Consumer record into the referral.

4. The Sending System requests the Author to validate the populated referral. 5. The Author reviews, edits and validates the information populated into the referral. 6. The Author completes the rest of the referral template, adding more information as required. 7. The Author saves a copy of the referral to the Consumer record and chooses the 'send' function in the Sending System. 8. The Sending System facilitates transmission of the referral to the Intended Recipient, and any additional Healthcare Services and/or Practitioner Roles by handing off message/s to a Relay System or Sending Edge Node.
Alternate flow of events
None identified

Functions Sequence	F10 Search for Intended Recipient F20 Select Intended Recipient F40 Generate Message, where the Message is a patient referral F50 Transmit Message to Intended Recipient

2.3.2. UC2 Send specialist letter

Description	During their management of a Consumer, the Author sends a specialist letter to one or more Healthcare Services and/or Practitioner Roles. The Author uses the specialist Sending System to create a new specialist letter (optionally based on a chosen template), incorporate electronic data, adds one or more Healthcare Services and/or Practitioner Roles as recipients, adds or updates additional data manually and sends the specialist letter. In this context, the Author is the healthcare provider with the responsibility for the information set out in the letter some of which may have sourced/supplied by other personnel.
Use Case #	UC2
Goal	To create a specialist letter and send it to the` nominated Healthcare Service(s) and/or or Practitioner Role(s).
Primary Actor	Author
Other Actors	Consumer Sending System Provider Directory
Assumptions	The Author has commenced/completed the required treatment of the Consumer as per a received referral request.
Pre-conditions	The Author determines that there is sufficient reason to send a specialist letter to the Healthcare Service(s) and/or Practitioner Role(s).

Triggers	The Author has completed a course of treatment for the Consumer, or there has been a development in the Consumer's clinical situation, such that the Author decides that there is a need to write and send a specialist letter.
Basic flow of events	
1. The Author uses the Sending System to select the desired template for the specialist letter. 2. The Sending System checks whether the Intended Recipient supports the chosen payload format. 3. The Sending System populates relevant information into desired fields of the template from the Consumer record. 4. The Author validates the populated information. 5. The Author edits/updates the populated information if required. 6. The Author selects one or more Healthcare Services and/or Practitioner Roles to send the specialist letter to (e.g., the Consumer's usual general practitioner) 7. The Author searches a Provider Directory for a Healthcare Service or Practitioner Role as recipient. 8. The Author selects the Healthcare Service or Practitioner Role from the search results. 9. The Sending System adds them to the distribution list. 10. The author may repeat the process to add additional Healthcare Services or Practitioner Roles that the message will be delivered to. 11. The Author enters remaining information as clinically required. 12. The Author completes the letter. 13. The Author saves a copy of the letter to the patient record and chooses the 'send' function in the Sending System. 14. The Sending System facilitates delivery of the specialist letter to the Healthcare Services and/or Practitioner Roles in the distribution list.	
Alternate flow of events	
4. If the Author has chosen an existing referral to respond to, the Sending System automatically populates the referring Healthcare Service or Practitioner Role details from the selected referral.	
Post-conditions	The Sending System has a completed specialist letter and initiated its transmission to the Healthcare Service(s) and/or Practitioner Role(s) on the distribution list.
Functions Sequence	F10 Search for Intended Recipient F20 Select Intended Recipient F40 Generate Message, where the Message is a specialist letter F50 Transmit Message to Intended Recipient

2.3.3. UC3 Send discharge summary

Description	The Sending System creates a new discharge summary for a Consumer on demand. The Sending System is used to incorporate electronic data, identify one or more Healthcare Services and/or Practitioner Roles as recipients, and add or update data manually before choosing to release the discharge summary (either in interim, final or amended form) to be sent.
Use Case #	UC3
Goal	To send a discharge summary to the Healthcare Services and/or Practitioner Roles in the distribution list.
Primary Actor	Author
Other Actors	Consumer Sending System Provider Directory
Assumptions	None
Pre-conditions	The Consumer has been admitted to the hospital.
Triggers	The Sending System receives a notification of the Consumer's admission and has determined that they will require a discharge summary (based on hospital/ward/unit specific rules).
Basic flow of events	
1. The Sending System creates a new discharge summary on demand, populates it with any required information supplied from other feeder systems, and assigns it to the Author. 2. The Author searches a Provider Directory for and adds one or more Healthcare Services and/or Practitioner Roles to the discharge summary's distribution list: a. The Author searches a Provider for a Healthcare Service or Practitioner Role. b. The Author selects one or more from the search results to be recipients. c. The discharge summary system adds the Healthcare Service(s) and/or Practitioner Role(s) to the distribution list. d. The Author may repeat the process to add additional Healthcare Services or Practitioner Roles that the message will be delivered to. 3. The feeder systems continue to supply the latest clinical information to the discharge summary system during the Consumer's stay in hospital. The Author chooses to incorporate relevant information into the discharge summary (including manually entered information as necessary). 4. Before the hospital discharges the Consumer, the Author reviews the discharge summary to ensure it that it contains the most current and relevant information, and confirms the distribution list, before marking it as complete and authorising its distribution. 5. The Sending System facilitates delivery of the specialist letter to the Healthcare Services and/or Practitioner Roles in the distribution list.	
Alternate flow of events	

4. The Author is releasing an interim discharge summary: a. The Author authorises the discharge summary for release with a status of 'Interim'. 4. The Author is releasing a final discharge summary: a. The Author authorises the discharge summary for release to all recipients who received the interim discharge summary, with a status of 'Final'. 4. The Author is releasing an amended version of a discharge summary: a. The Author authorises the discharge summary for release to all recipients who received the final discharge summary, with a status of 'Amended'.	
Post-conditions	The Sending System has a completed discharge summary and initiated its transmission to the Healthcare Service(s) and/or Practitioner Role(s) on the distribution list.
Functions Sequence	F10 Search for Intended Recipient F20 Select Intended Recipient F30 Authenticate Intended Recipient F40 Generate Message, where the Message is a discharge summary F50 Transmit Message to Intended Recipient

2.3.4. UC4 Send diagnostic order

Description	During their management of a Consumer, the Author may decide that the Consumer requires a diagnostic service such as a pathology or imaging test. The Author uses the Sending System to create a new order (based on a chosen template), incorporate electronic data, identify a Healthcare Service to send the order to, and add or update additional data manually.
Use Case #	UC4
Goal	To send a diagnostic order to the Healthcare Services in the distribution list.
Primary Actor	Author
Other Actors	Consumer Sending System Provider Directory
Assumptions	None
Pre-conditions	None
Triggers	With Consumer consent, the Author decides to order a laboratory test for the Consumer.
Basic flow of events	

1. In consultation with the Consumer, the Author searches for and chooses a Diagnostic Healthcare Service to send the order to: a. The Author searches a Provider Directory for a Healthcare Service that can execute the order. b. The Author selects the Healthcare Service from the search results. c. The Sending System adds the Healthcare Service to the distribution list. d. The Author may repeat the process to add additional Healthcare Services or Practitioner Roles that the message will be delivered to. 2. The Author opens the correct order template in the Sending System. a. The Sending System checks whether the Intended Recipient supports the chosen payload format. 3. The Sending System populates available information from the Consumer's record. 4. The Sending System requests the Author to validate the populated information. 5. The Author reviews, edits and validates the populated information in the order. 6. The Author completes the rest of the order template, adding more information if required. 7. The Author saves a copy of the order to the Consumer record and chooses the 'send' function in the Sending System. 8. The Sending System facilitates delivery of the diagnostic order to the Healthcare Service in the distribution list.	
Alternate flow of events	
None identified	
Post-conditions	The Sending System has a completed diagnostic order and initiated its transmission to the Healthcare Service on the distribution list.
Functions Sequence	F10 Search for Intended Recipient F20 Select Intended Recipient F40 Generate Message, where the Message is a diagnostic order F50 Transmit Message to Intended Recipient

2.3.5. UC5 Send diagnostic result

Description	A Consumer has undergone a diagnostic service such as a pathology or imaging test, and the Author sends the results to one or more Healthcare Service or Practitioner Roles (e.g., the GP that made the original diagnostic order). The Author uses the Sending System to create the diagnostic result document, incorporate electronic data, add recipients, and add or update additional data manually.
Use Case #	UC5
Goal	To send a diagnostic result report to the Healthcare Services and/or Practitioner Roles in the distribution list.

Primary Actor	Author
Actors	Consumer Sending System Provider Directory
Assumptions	The Sending System has a diagnostic order containing the requesting Healthcare Service or Practitioner Role's details.
Pre-conditions	None identified
Triggers	The requested diagnostic service (such as a pathology or imaging test) has been completed and the results are available within the Sending System.
Basic flow of events	
1. The Sending System adds the requesting Healthcare Service or Practitioner Role (from the original order) to the list of recipients, and optionally additional recipients: a. The Author searches a Provider Directory for Healthcare Services and/or Practitioner Roles. b. The Author selects them from the search results. c. The Sending System adds them to the distribution list. d. The Author may repeat the process to add additional Healthcare Services or Practitioner Roles that the message will be delivered to. 2. The Author opens the correct results report template in the Sending System. 3. The Sending System populates available information from the Consumer record, including test results. 4. The Sending System requests the Author to validate the populated information. 5. The Author reviews, edits and validates the populated information in the results. 6. The Author completes the rest of the results report, adding more information if required. 7. The Author saves a copy of the results report to the Consumer record and chooses the 'send' function in the Sending System. 8. The Sending System facilitates delivery of the diagnostic result to the Healthcare Services and/or Practitioner Roles in the distribution list.	
Alternate flow of events	
None identified	
Post-conditions	The Sending System has a completed results report and initiated its transmission to the Healthcare Service(s) and/or Practitioner Role(s) on the distribution list.
Functions Sequence	F10 Search for Intended Recipient F20 Select Intended Recipient F40 Generate Message, where the Message is a diagnostic result F50 Transmit Message to Intended Recipient

2.3.6. UC6 Store and acknowledge received Clinical Message

Description	A Receiving System has received a Clinical Message (referral, specialist letter, etc) **stored** it and sends an Accept Acknowledgement Message to the Sending System to acknowledge it has been received.
Use Case #	UC6
Goal	To **store** a received Clinical Message and create an Accept Acknowledgement Message to the Sending System.
Primary Actor	Receiving System
Other Actors	Sending System
Assumptions	The received Clinical Message follows one of the accepted message formats defined in Appendix A. The received Clinical Message can be processed sufficiently to create the Accept Acknowledgement Message by the Receiving System.
Pre-conditions	The Receiving System has received a Clinical Message which needs to be reviewed, processed clinically and acknowledged.
Triggers	The Receiving System receives and stores a Clinical Message.
Basic flow of events	
1. The Receiving System receives and stores a Clinical Message. 2. The Receiving System generates an Accept Acknowledgement Message. 3. The Receiving System populates the Accept Acknowledgement Message using information from the received Clinical Message, and from the Receiving System. 4. The Receiving System facilitates the transmission of the Accept Acknowledgement Message back to the Sending System.	
Alternate flow of events	
3. The received Clinical Message cannot be processed sufficiently to create the Accept Acknowledgement Message, so the failure is brought to the attention of a Responsible Person for investigation and resolution.	
Post-conditions	The Receiving System has a stored the Clinical Message and initiated the send of an Acknowledgement to the Sending System.
Functions Sequence	F60 Process Message F70 Authenticate Sender, confirm Message integrity F90 Detect duplicate Messages F40 Generate Message, where the Message is an Accept Acknowledgement Message F50 Transmit Message to Intended Recipient

2.3.7. UC7 Process and acknowledge received Clinical Message

Description	A Receiving System has received a Clinical Message (referral, specialist letter, etc) **processed** it and sends an Application Acknowledgement Message to the Sending System to acknowledge it has been processed.
Use Case #	UC7
Goal	To **process** a received Clinical Message and send an Application Acknowledgement Message to the Sending System.
Primary Actor	Receiving System
Other Actors	Sending System
Assumptions	The received Clinical Message follows one of the accepted message formats defined in Appendix A. The received Clinical Message has been successfully stored by the Receiving System, and it can now be processed sufficiently to create the Application Acknowledgement Message.
Pre-conditions	The Receiving System has received a Clinical Message ready to be processed and acknowledged.
Triggers	The Receiving System processes a received Clinical Message.
Basic flow of events	
1. The Receiving System processes a stored Clinical Message that it has previously received. 2. The Receiving System generates an Application Acknowledgement Message. 3. The Receiving System populates the Application Acknowledgement Message using information from the received Clinical Message, and from the Receiving System. 4. The Receiving System facilitates the transmission of the Application Acknowledgement Message back to the Sending System.	
Alternate flow of events	
None identified	
Post-conditions	The Receiving System has a processed the Clinical Message and initiated the send of an Application Acknowledgement to the Sending System.
Functions Sequence	F40 Generate Message, where the Message is an Application Acknowledgement (e.g., RRI-I12) F50 Transmit Message to Intended Recipient

2.3.8. UC8 Process received Acknowledgement Message

Description	The Sending System receives and processes an Accept Acknowledgement Message or an Application Acknowledgement Message from the Receiving System.

Use Case #	UC8
Goal	To process a received Acknowledgment Message so that the Author of the corresponding Clinical Message, administrative users, etc can identify the status of the message exchange process.
Primary Actor	Receiving System
Other Actors	None
Assumptions	The received Acknowledgement Message follows one of the accepted message formats defined in Appendix A. The received Acknowledgement Message can be processed by the Receiving System.
Pre-conditions	None
Triggers	The Receiving System receives an Acknowledgement Message.
Basic flow of events	
1. The Receiving System receives an Accept Acknowledgement Message or an Application Acknowledgement Message. 2. The Receiving System processes the Message. 3. The Receiving System links the received Acknowledgement Message to a corresponding sent Clinical Message. 4. The Receiving System updates the status of the Clinical Message with one of the following statuses to support the message reconciliation process (see UC9): a. Accepted (original Clinical Message has been accepted) b. Rejected (original Clinical Message has been rejected) c. Error (an error was encountered when processing the original Clinical Message)	
Alternate flow of events	
3a. The received Acknowledgement Message cannot be linked to a sent Clinical Message, so it is brought to the attention of a Responsible Person for investigation and resolution.	
Post-conditions	The status of a sent Clinical Message has been updated.
Functions Sequence	F60 Process Message F70 Authenticate Sender, confirm Message integrity F90 Detect duplicate Messages

2.3.9. UC9 Identify status of message

Description	A. An Author (or Administrator) wants to track the status of a *sent* Clinical Message. They want to determine whether it has been sent, received by the Receiving System, acknowledged (with an Accept, Error or Reject indicator), or expired. B. An Intended Recipient (or Administrator) wants to track the status of a *received* Clinical Message. They want to determine whether an Application

	Acknowledgement has been successfully delivered back to the Sending Edge Node.
Use Case #	UC9
Goal	To check the status of a Message.
Actors	A. Author (or Administrator) + Sending System B. Intended Recipient (or Administrator) + Receiving System
Assumptions	Messages for which the statii are being checked have been successfully stored by the system being used.
Pre-conditions	A. A Clinical Message has been sent. B. A Clinical Message has been received.
Triggers	A. An Author (or Administrator) logs into the Sending System and navigates to a screen that offers Message reconciliation functionality. B. An Intended Recipient (or Administrator) logs into the Receiving System and navigates to a screen that offers Message reconciliation functionality.
Basic flow of events	
An Author (or Administrator) logs into the Sending System and navigates to a screen that offers Message reconciliation functionality. (B) An Intended Recipient (or Administrator) logs into the Receiving System and navigates to a screen that offers Message reconciliation functionality. This may involve: • accessing a Consumer-centric screen (showing only Messages that pertain to a particular Consumer) • accessing a more general or administrative screen that enables all Messages to be viewed • searching, filtering or selecting a subset of Messages available the System • the actor determines the status of the Message(s) of interest	
Alternate flow of events	
None identified	
Post-conditions	The actor knows the status of Messages of interest.
Functions Sequence	F100 Reconcile Messages

2.4. Functions and Requirements

2.4.1. F10 Search for Intended Recipient

This function enables authorised Authors to search for Intended Recipients from an identified Provider Directory.

2.4.1.1. R10 Search supported

Requirement #	R10
Requirement Name	Search supported
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL enable Authors to search for Intended Recipients.
Notes	

2.4.1.2. R20 Authorised searching only

Requirement #	R20
Requirement Name	Authorised searching only
Requirement Type	Non-Functional
Optionality	MANDATORY
Requirement	The solution SHALL allow only Authorised Users to execute searches for Intended Recipients.
Notes	

2.4.2. F20 Select Intended Recipient

This function enables authorised Authors to select an appropriate Intended Recipient from an identified Provider Directory.

2.4.2.1. R40 Intended Recipient identifiable

Requirement #	R40
Requirement Name	Intended Recipient identifiable
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL display sufficient information to enable Authors (in consultation with the Consumer) to select the correct/desired Intended Recipient.
Notes	

2.4.2.2. R50 Intended Recipient supports secure messaging

Requirement #	R50

Requirement Name	Intended Recipient supports secure messaging
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL ensure only Intended Recipients capable of receiving Messages transmitted via the NSMN are allowed to be selected as Intended Recipients (for Messages being transmitted via the NSMN) unless the user is informed of the risk and overrides.
Notes	

2.4.2.3. R60 Intended Recipient details current

Requirement #	R60
Requirement Name	Intended Recipient details current
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL ensure details of Intended Recipient are up to date prior to send.
Notes	This mainly pertains records copied to a Local Address Book, then re-used.

2.4.3. F30 Authenticate Intended Recipient

This function enables Authors to take steps to ensure they have correctly identified the Intended Recipient.

2.4.3.1. R70 Intended Recipient confirmed

Requirement #	R70
Requirement Name	Intended Recipient confirmed
Requirement Type	Functional
Optionality	MANDATORY
Requirement	Before sending a Message, the solution SHALL take steps to confirm the identity of the Intended Recipient in order to protect patient privacy.
Notes	

2.4.4. F40 Generate Message

This function enables the Sending System to create an electronically transmittable message that can be processed and understood by the Receiving System.

2.4.4.1. R80 Messages interoperable

Requirement #	R80
Requirement Name	Messages interoperable
Requirement Type	Non-Functional
Optionality	MANDATORY
Requirement	The solution SHALL create Message formats able to be processed and understood by Receiving Systems.
Notes	

2.4.4.2. R90 Messages uniquely identifiable

Requirement #	R90
Requirement Name	Messages uniquely identifiable
Requirement Type	Non-Functional
Optionality	MANDATORY
Requirement	The solution SHALL ensure all Messages can be uniquely identified by all NSMN Participants (Clients, Edge Nodes, and Core Nodes).
Notes	

2.4.4.3. R100 Message datetimes identifiable

Requirement #	R100
Requirement Name	Message datetimes identifiable
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL enable accurate determination of dates and times pertaining to Messages.
Notes	HL7 standard date/time formats are to be used in Clinical Messages. Refer to the HL7 Timestamp Specification All dateTime fields in a Sealed Message shall be transmitted as timezoned values in the UTC timezone as defined in ATS-5822 Section 2.5 p9.

2.4.5. F50 Transmit Message to Intended Recipient

This function enables the Sending System and Sending Edge Node to transmit the Message to the Intended Recipient.

2.4.5.1. R110 Messages transmittable

Requirement #	R110
Requirement Name	Messages transmittable
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL support the transmission of Messages.
Notes	

2.4.5.2. R120 Sending System must be able to receive Message Acknowledgement

Requirement #	R120
Requirement Name	Sending System must be able to receive Message Acknowledgement
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL NOT transmit Clinical Messages if the Sending System is unable to receive corresponding Acknowledgements.
Notes	Recipient supported Payload types must be declared in the Secure Message Endpoint Resource in the Provider Directory.

2.4.5.3. R130 Delivery re-try

Requirement #	R130
Requirement Name	Delivery re-try
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL support retry of failed delivery of a Message as it was created.
Notes	

2.4.5.4. R140 Messages have expiry time

Requirement #	R140

Requirement Name	Messages have expiry time
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The Sending Edge Node SHALL enable specifying a Message expiry time.
Notes	The use case defines a transport level expiry and not a clinical level expiry (such as an expiry date of a referral).

2.4.5.5. R150 Messages not transmitted after expiry

Requirement #	R150
Requirement Name	Messages not transmitted after expiry
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The Sending Edge Node SHALL not transmit Messages after they have expired.
Notes	

2.4.5.6. R160 Delivery must be reliable

Requirement #	R160
Requirement Name	Delivery must be reliable
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL enable Authors to reliably ascertain which Messages have been successfully delivered and which have not.
Notes	

2.4.6. F60 Process Message

This function enables a received Message to be processed by the Receiving System.

2.4.6.1. R170 Received Messages are able to be processed

Requirement #	R170
Requirement Name	Received Messages are able to be processed
Requirement Type	Functional

Optionality	MANDATORY
Requirement	Receiving Systems SHALL be able to process received Messages that are declared as supported Payload types in the Provider Directory.
Notes	

2.4.6.2. R180 Received Messages accurately presented for action

Requirement #	R180
Requirement Name	Received Messages accurately presented for action
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL ensure that received Messages are made available to an application and accurately presented to an individual to take appropriate action in relation to the Message.
Notes	See the guidelines set out at Formatting Pathology Reports and SPIA Rendering of numerics.

2.4.6.3. R190 Receiving System must be able to generate and send Message Acknowledgement

Requirement #	R190
Requirement Name	Receiving System must be able to generate and send Message Acknowledgement
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL acknowledge receipt of Clinical Messages by the Receiving System by generating and sending Acknowledgement Messages to the Sending System.
Notes	

2.4.7. F70 Authenticate Sender, confirm Message integrity

This function enables the Intended Recipient to authenticate the Sender and confirm that the received Message has not been tampered with.

2.4.7.1. R200 Sender authenticated

Requirement #	R200
Requirement Name	Sender authenticated

Requirement Type	Functional
Optionality	MANDATORY
Requirement	Receiving Edge Node SHALL authenticate the Sender.
Notes	

2.4.7.2. R220 Message integrity confirmed

Requirement #	R220
Requirement Name	Message integrity confirmed
Requirement Type	Functional
Optionality	MANDATORY
Requirement	Receiving Edge Node SHALL confirm the integrity of received Messages (i.e. they have not been tampered with). This should include verifying that the sending facility content is consistent with the signing party.
Notes	

2.4.8. F90 Detect duplicate Messages

This function enables the Receiving System to detect duplicate received Messages, so they are not incorrectly processed.

2.4.8.1. R240 Duplicate Messages detected

Requirement #	R240
Requirement Name	Duplicate Messages detected
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The Receiving System SHALL ensure duplicate Messages are identified and handled appropriately.
Notes	

2.4.9. F100 Reconcile Messages

This function enables Authors to :

- Ascertain which sent Clinical Messages have received Acknowledgements; and
- Enables Intended Recipients to ascertain which receiving Clinical Messages their Receiving System has sent Acknowledgement Message(s) for.

2.4.9.1. R250 Authors able to reconcile Messages

Requirement #	R250
Requirement Name	Authors able to reconcile Messages
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL enable Authors to identify which sent Messages have received Acknowledgements (including differentiating acknowledgements that indicate *accepted, rejected* or *error* conditions).
Notes	

2.4.9.2. R260 Intended Recipients able to reconcile Messages

Requirement #	R260
Requirement Name	Intended Recipients able to reconcile Messages
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL enable Intended Recipients to identify which Messages their Receiving System have acknowledged (including differentiating *accepted, rejected* or *error acknowledgements*).
Notes	

2.4.10. General requirements

2.4.10.1. R300 Messages protected in transit

Requirement #	R300
Requirement Name	Messages protected in transit
Requirement Type	Functional
Optionality	MANDATORY
Requirement	Messages SHALL be protected from unauthorised access in transit.
Notes	

2.4.10.2. R310 No unauthorised access to Messages

Requirement #	R310

Requirement Name	No unauthorised access to Messages
Requirement Type	Functional
Optionality	MANDATORY
Requirement	The solution SHALL ensure that received Messages are handled in a manner that prevents unauthorized access to the content of the Message.
Notes	

3. NSMN Solution Requirements

3.1. NSMN Solution Requirements

This section contains the NSMN Interoperability Specification Solution Requirements, or "Solution Requirements" for short. The purpose of the Solution Requirements, and their place within the NSMN Interoperability Specification, are described in section 1.1.

3.2. Structure of the Solution Requirements

The Solution Requirements are divided into two parts:

3.2.1. Blueprint

The NSMN Blueprint provides technical information about the NSMN solution. Whereas the Interoperability Requirements are structured around a set of *business roles* (e.g., Author, Intended Recipient) and the use-cases they wish to execute (e.g., Send a referral, Reconcile Messages, etc), these Solution Requirements are structured around a set of *five roles* - Sending System, Sending Edge Node, Core Node, Receiving Edge Node, Receiving System and Provider Directory.

These roles are defined in the NSMN Blueprint. Each solution participating in the NSMN will declare their intention to fulfill one or more of these roles. For example, a GP Practice software solution may declare that they intend to fulfill the Sending System and Receiving System roles. In doing so, they will be able to identify which parts of the Solution Guidelines apply to them, and thus what requirements and solution constraints their systems must meet to participate in the NSMN.

3.2.2. Guidelines

The NSMN Solution Guidelines make up the second part of this Solution Requirements and are contained in sections 3.3 to 3.9 of this document. The Solution Guidelines are structured around the roles defined in the Blueprint. For each solution role (e.g. Sending System), there is a corresponding section in the Solution Guidelines which specifies which requirements from the Conformance Requirements the solution must meet to fulfill the role[1]. For some of these requirements, the solution fulfilling the role will be free to build any solution that meets the requirement.

For example, referring to RSC-SS80 Intended Recipient details current, a requirement that Intended Recipient details must be confirmed to be up to date before use, must be met by all Sending Systems. However, there is no associated Solution Constraint, meaning Sending Systems can meet this requirement using whatever solution they deem fit.

[1] Each requirement in the National Base Profile's Conformance Requirements must be allocated to at least one solution role. It may be allocated to multiple solution roles.

For other requirements, there will be a *solution constraint* that constrains the way the solution must be built.

For example, RSC-SS20 Use of Public Key Infrastructure for authentication, a requirement for all systems searching Provider Directories to present authentication credentials, applies to all Sending Systems. Moreover, the presence of a solution constraint means that Sending Systems must meet this requirement through a particular solution – authenticate using PKI when connecting to other systems.

3.3. Requirements and solution constraints: Sending Systems

3.3.1. RSC-SS10 Sending Systems able to search Provider Directory

RSC #	RSC-SS10
RSC Name	Sending Systems able to search Provider Directory
Requirement	*R10 Search supported*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	Sending Systems SHALL be able to search a Core Node Provider Directory to enable Authors to identify potential Intended Recipients. The system SHALL support all search capabilities that are specified as "MUST support" in the profiles section of the Australian Provider Directory Implementation Guide. This includes navigation of paged results from Provider Directories (refer to section 3.8.5 RSC-PD50 Provider Directory Support paging result sets).
Notes	

3.3.2. RSC-SS20 Use of Public Key Infrastructure for authentication

RSC #	RSC-SS20
RSC Name	Use of Public Key Infrastructure for authentication
Requirement	*R20 Authorised searching only*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	Authentication: When connecting to the Provider Directory over a public network,

	the Sending System SHALL authenticate the identity of the Provider Directory using Public Key Infrastructure (PKI). Assert Identity: When connecting to the Provider Directory over a public network, the Sending System SHALL assert the identity of the organisation operating the system to the Provider Directory.
Notes	See Appendix B – Approved Certificate Authorities. Other authentication and authorization protocols MAY be used if both the Sending System and Provider Directory agree.

3.3.3. RSC-SS40 Intended Recipient identifiable

RSC #	RSC-SS40
RSC Name	Intended Recipient identifiable
Requirement	*R40 Intended Recipient identifiable*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	The Sending System SHALL populate MSH-4 with the Sending Facility as specified in Section 2.1.9.4 of the Australian Diagnostics and Referral Messaging – Localisation of HL7 Version 2.4. The Sending System SHALL also populate MSH-6 with the Receiving Facility as specified in Section 2.1.9.6 of the Australian Diagnostics and Referral Messaging – Localisation of HL7 Version 2.4. The message header elements MSH-4 and MSH-6 SHALL be validated against the Provider Directory.
Notes	

3.3.4. RSC-SS50 Intended Recipient has a Receiving Edge Node

RSC #	RSC-SS50
RSC Name	Intended Recipient has a Receiving Edge Node
Requirement	*R50 Intended Recipient supports secure messaging*
Applies to Role	Sending Systems
Optionality	MANDATORY

Solution Constraint	If the Sender is using the Local Address Book then the Sending System SHALL confirm that • the Recipient entry exists in the Provider Directory • has a Receiving Edge Node with an Endpoint; and • The cached copy is completely valid If the Recipient's Endpoint is not found in the Provider Directory or there is no Receiving Edge Node for the Recipient, then the Sending System MAY issue a warning to the user and provide an option to send it anyway.
Notes	

3.3.5. RSC-SS60 Receiving Edge Node connectivity type is correct

RSC #	RSC-SS60
RSC Name	Receiving Edge Node Connection Type is correct
Requirement	*R50 Intended Recipient supports secure messaging*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	a. Sending Systems SHALL check the destination Endpoint's Connection Type, as retrieved from the Provider Directory, has the value for Secure Message Delivery (Deferred Mode) as defined in the Australian Secure Message Service Interfaces ValueSet. b. The value is: http://ns.electronichealth.net.au/smd/intf/SealedMessageDelivery/TLS/2010 When the Connection Type cannot be retrieved from the Provider Directory or it is not the valid value for Secure Message Delivery (Deferred Mode), the Sending System SHALL provide a warning to the user. The Sending System MAY enable the user to accept the risk, override and send it anyway.
Notes	

3.3.6. RSC-SS70 Receiving Edge Node Payload type correct

RSC #	RSC-SS70
RSC Name	Receiving Edge Node Payload Type correct

Requirement	*R50 Intended Recipient supports secure messaging*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	The Sending System SHALL confirm that the destination Endpoint can receive the Payload Type of the Message being sent. If the Payload Type cannot be retrieved from the Provider Directory or it has an invalid value, the Sending System SHALL provide a warning to the user. The warning MAY enable the user to accept the risk, override and send it anyway.
Notes	The Endpoint's Payload Types are found in the Provider Directory element: Endpoint.payloadType as defined in the Australian Secure Messaging Endpoint Directory Entry Endpoint.payloadType.

3.3.7. RSC-SS80 Intended Recipient details current

RSC #	RSC-SS80
RSC Name	Intended Recipient details current
Requirement	*R60 Intended Recipient details current*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	An Intended Recipient's details retrieved from a Local Address Book SHALL be verified against the Provider Directory, and updated if necessary, prior to the Message being sent.
Notes	All mandatory elements from the Provider Directory SHOULD be matched and updated with the Local Address Book details.

3.3.8. RSC-SS90 Standard Message formats

RSC #	RSC-SS90
RSC Name	Standard Message formats
Requirement	*R80 Messages interoperable*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	Sending Systems SHALL produce Messages in standard formats – see Appendix A.

Notes	

3.3.9. RSC-SS91 Message control identifier must be unique

RSC #	RSC-SS91
RSC Name	Message control identifier format
Requirement	*R90 Messages uniquely identifiable*
Applies to Role	Sending System
Optionality	MANDATORY
Solution Constraint	Sending Systems MUST use a unique identifier over time for their system instance.
Notes	The following format for the Message Control Identifier (MSH-10) as per 2.9.10 MSH-10 Message control ID: <sending facility>_<date>.n{nnnnnnn..} could be used. Australian variation to HL7 V2.4 with the length changed from 20 to 36 characters to accommodate a globally unique identifier (GUID).

3.3.10. RSC-SS92 Standard Message formats for Message Categories

RSC #	RSC-SS92
RSC Name	Standard Message formats for Message Categories
Requirement	*R80 Messages interoperable*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	For each standard Clinical Message a Sending System supports, it SHALL produce the Message in the standard format as per the relevant specification referenced in the table in Appendix A.
Notes	

3.3.11. RSC-SS94 Support for Acknowledgement Messages for supported Clinical Messages

RSC #	RSC-SS94
RSC Name	Standard Message formats for Message Categories
Requirement	*R80 Messages interoperable*
Applies to Role	Sending Systems
Optionality	MANDATORY

Solution Constraint	For each standard Clinical Message a Sending System supports, it SHALL be able to receive and successfully process the associated Acknowledgement Messages.
Notes	

3.3.12. RSC-SS100 Non-standard Message formats

RSC #	RSC-SS100
RSC Name	Non-standard Message formats
Requirement	*R80 Messages interoperable*
Applies to Role	Sending Systems
Optionality	RECOMMENDED
Solution Constraint	If the Sending System supports a Clinical Message format that does not comply with the formats in Appendix A, it SHALL issue a warning. The Sending System MAY allow the user to accept the risk and send it anyway.
Notes	

3.3.13. RSC-SS110 Message size 16MB or less

RSC #	RSC-SS110
RSC Name	Message size 16MB or less
Requirement	*R80 Messages interoperable*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	The size of the Message SHALL NOT exceed 16 MB. The Sending System SHALL provide a warning message and MAY choose to send anyway.
Notes	Align with HL7 AU standard HL7au:000019

3.3.14. RSC-SS120 Correct timezone must be specified

RSC #	RSC-SS120
RSC Name	Correct timezone must be specified
Requirement	*R100 Message datetimes identifiable*

Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	All timestamp fields in a Clinical Message shall be transmitted as timezoned values as defined in 3 Datatypes - HL7AUSD-STD-OO-ADRM-2021.1 - HL7 Australia
Notes	

3.3.15. RSC-SS170 Alert – Notification of message not delivered

RSC #	RSC-SS170
RSC Name	Alert – Notification of message not delivered
Requirement	*R160 Delivery must be reliable*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	Sending Systems SHALL have method for bringing to the attention of a Responsible Person (refer RSC-G50 Escalation Pathway) the receipt of an error status from the Sending Edge Node indicating a Message has not been able to be delivered.
Notes	

3.3.16. RSC-SS180 Receipt of Application Acknowledgements

RSC #	RSC-SS180
RSC Name	Receipt of Application Acknowledgements
Requirement	*R160 Delivery must be reliable*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	Sending Systems SHALL be able to consume and interpret Application Acknowledgements (as specified in the HL7 Australia Acknowledgement Specification) as evidence of the success or failure of the message delivery process. Sending Systems MAY interpret other non-standard notifications as mutually agreed with the Sending Edge Node.

Notes	Application Acknowledgement codes are stated in MSA-1. "Systems upstream or users downstream from the target system, or the target system itself, may produce generic ACKs (|ACK|). This is because other segments in the message may be unreadable because of errors or they are unavailable to the processing system. This type of ACK is informational, the confirmation of delivery to the target system relies on the application ACK. These additional ACKs are accept ACKs as defined by the international standard." The MSA segment contains information that distinguishes between an accept ACK and application ACK. Accept ACKs MSA-1 values are prefixed with "C" whereas application ACKs are prefixed with "A" as per MSA segment.

3.3.17. RSC-SS190 Receipt of User Read Acknowledgement

RSC #	RSC-SS190
RSC Name	Receipt of User Read Acknowledgements
Requirement	*R160 Delivery must be reliable*
Applies to Role	Sending Systems
Optionality	RECOMMENDED
Solution Constraint	Sending Systems MAY receipt a User Read Acknowledgement
Notes	Sending Systems MAY be able to consume and interpret User Read Acknowledgements (as specified in HL7 Australia Acknowledgement Specification) as evidence that the user has read the Clinical Message.

3.3.18. RSC-SS220 Sign CDA Documents

RSC #	RSC-SS220
RSC Name	Sign CDA Documents
Requirement	*R200 Sender Authenticated* *R220 Message integrity confirmed*
Applies to Role	Sending Systems
Optionality	MANDATORY

Solution Constraint	When the Clinical Message is an outgoing Message that contains a CDA Document, the CDA Document SHALL be digitally signed by the Sending System with an X509v3 Certificate issued by an approved Certificate Authority (CA) – see Appendix B. Refer to Section 4 of the Clinical Documents – CDA Package v1.0 for specifications for signing the message.
Notes	

3.3.19. RSC-SS240 Authors able to reconcile Messages

RSC #	RSC-SS240
RSC Name	Authors able to reconcile Messages
Requirement	*R250 Authors able to reconcile Messages*
Applies to Role	Sending Systems
Optionality	MANDATORY
Solution Constraint	Sending Systems SHALL provide a mechanism to keep track of the status of each Clinical Message. Sending Systems SHALL provide a mechanism to inform the user of the status of each Clinical Message they have sent.
Notes	

3.4. Requirements and solution constraints: Sending Edge Nodes

3.4.1. RSC-SEN10 Use of Public Key Infrastructure for authentication

RSC #	RSC-SEN10
RSC Name	Use of Public Key Infrastructure for authentication
Requirement	*R20 Authorised searching only*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Authentication: When connecting over a public network to the Provider Directory, Sending System or Core Node, the Sending Edge Node SHALL

	authenticate the identity of the entity to which it is connecting using Public Key Infrastructure (PKI). Assert Identity: When connecting over a public network to the Provider Directory, Sending System, or Core Node, the Sending Edge Node SHALL assert the identity of the organisation operating it to the entity to which it is connecting.
Notes	

3.4.2. RSC-SEN20 Sending Edge Node to check Public Key Certificate

RSC #	RSC-SEN20
RSC Name	Sending Edge Node to check Public Key Certificate
Requirement	*R70 Intended Recipient confirmed*
Applies to Role	Sending Edge Node
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL validate the authenticity of the Intended Recipient's Public Key Certificate (retrieved from the Provider Directory) against the trusted Certificate Authority (CA). The Public Key Certificate needs to be current (i.e., not expired) and signed by the CA's Private Key. When these checks fail, the Message MUST NOT be transmitted.
Notes	ATS-5822 Section 3.3.5 (a) p15 "The Sender shall initially validate the authenticity of Intended Recipient encryption certificates. These certificates will usually be returned with a service directory record or retrieved through certificate references returned with the service directory record."

3.4.3. RSC-SEN30 Compare identifiers in Public Key Certificate and Endpoint

RSC #	RSC-SEN30
RSC Name	Compare identifiers in Certificate and Endpoint
Requirement	*R70 Intended Recipient confirmed*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY

Solution Constraint	Sending Edge Nodes SHALL confirm the identifier in the Intended Recipient's Public Key Certificate (retrieved from the Provider Directory) matches one of the identifiers for the destination Endpoint. Where the check fails, the Message MUST NOT be transmitted.
Notes	ATS-5822 Section 3.3.5 (b) p15 "The Sender should validate that the identity information contained in the Certificate matches local identity information for the Receiver or identifies a Responsible Person for the Receiver. The validation shall be sufficient to ensure that the privacy obligations of the Sender are satisfied. The Sender shall not send a Message if their privacy obligations relating to the Message are not satisfied. Privacy obligations are defined in the Commonwealth Privacy Act [PRV1988] and in relevant state and territory legislation. Further information about privacy legislation and principles relevant to e-health is provided in [NPRV2006]."

3.4.4. RSC-SEN40 Sending Edge Node to establish Message expiry time

RSC #	RSC-SEN40
RSC Name	Sending Edge Node to establish Message expiry time
Requirement	*R140 Messages have expiry time*
Applies to Role	Sending Edge Node
Optionality	MANDATORY
Solution Constraint	Sending Edge node SHALL establish the expiry time and populate the appropriate field in the Secure Message data as defined in Section 7.3.2 of ATS-5822.
Notes	

3.4.5. RSC-SEN50 No re-try after Message expiry

RSC #	RSC-SEN50
RSC Name	No re-try after Message expiry
Requirement	*R150 Messages not transmitted after expiry*
Applies to Role	Sending Edge Node
Optionality	MANDATORY

Solution Constraint	Sending Edge Node SHALL NOT retry delivery invocation after the Sealed Message expiry time.
Notes	ATS-5822 Section 3.3.6 (a) p16 "The expiryTime is inserted in the Sealed Message by the Sending Edge Node as specified in Section B2.3 of ATS-5822 (p56)."

3.4.6. RSC-SEN55 Notify Sending System on expiry

RSC #	RSC-SEN55
RSC Name	Notify Sending System on expiry
Requirement	*R150 Messages not transmitted after expiry*
Applies to Role	Sending Edge Node
Optionality	MANDATORY
Solution Constraint	The Sending Edge Node SHALL notify the Sending System if a message has expired.
Notes	ATS-5822 Section 3.3.6 (a) p16 "Failure in setting the expiryTime or a Message not delivered by the expiryTime is to be communicated using HL7 v2 ACK with AE code, or an alternative mechanism as agreed between the Sending Edge Node and Sending System."

3.4.7. RSC-SEN80 Sending Edge Nodes create Sealed Messages

RSC #	RSC-SEN80
RSC Name	Sending Edge Nodes create Sealed Messages
Requirement	*R80 Messages interoperable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL construct Sealed Messages in accordance with Section 7.3 of the ATS-5822 standard, and XML Schema described in Section 2.3 of the ATS-5821 standard.
Notes	ATS-5822 Section 1.6 p7

3.4.8. RSC-SEN90 Invocation Identifier format

RSC #	RSC-SEN90

RSC Name	Invocation Identifier format
Requirement	*R90 Messages uniquely identifiable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL use the following formats for the Invocation (or Response) Identifier as per ATS-5822 section 2.6.3. 1) a UUID encoded as a URN according to RFC 4122; or 2) a URL based on a domain name registered by the creating Endpoint, and an identifier that is unique at the creating Endpoint.
Notes	For more information refer to RFC 4122

3.4.9. RSC-SEN100 Do not re-use Invocation Identifiers

RSC #	RSC-SEN100
RSC Name	Do not re-use Invocation Identifiers
Requirement	*R90 Messages uniquely identifiable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL not re-use Invocation Identifiers unless retrying a failed invocation.
Notes	ATS-5822 Section 3.3.6 (b), (d) p16

3.4.10. RSC-SEN110 Datetimes to be UTC

RSC #	RSC-SEN110
RSC Name	Datetimes to be UTC
Requirement	*R100 Message datetimes identifiable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	All dateTime fields in a Sealed Message shall be transmitted as timezoned values in the UTC timezone as defined in ATS-5822 Section 2.5 p9.

Notes	Note that this constraint applies only to elements in the XML Schema Definition of the Message and not to the Payload.

3.4.11. RSC-SEN120 Receive Messages from Sending System

RSC #	RSC-SEN120
RSC Name	Receive Messages from Sending System
Requirement	*R110 Messages transmittable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL have a mechanism to receive Clinical Messages from a Sending System.
Notes	**File Drop:** The exchange of standard HL7 V2 payloads via a local file system is a common convention for the exchange of messages between Edge Nodes and Clients.

3.4.12. RSC-SEN130 Transmit Messages to Core Node

RSC #	RSC-SEN130
RSC Name	Transmit Messages to Core Node
Requirement	*R110 Messages transmittable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL have a mechanism to transmit Sealed Messages to a Core Node.
Notes	ATS-5822 Section 5.2 provides a reliable, secure mechanism for this purpose. However, other proprietary mechanisms MAY be used.

3.4.13. RSC-SEN140 Sending Edge Node must receive and process Acknowledgements

RSC #	RSC-SEN140
RSC Name	Sending Edge Node must receive and process Acknowledgements
Requirement	*R120 Sending System must be able to receive Message Acknowledgements*
Applies to Role	Sending Edge Nodes

Optionality	MANDATORY
Solution Constraint	For each standard Clinical Message the Sending Edge Node supports, it SHALL be able to receive and successfully process the associated Acknowledgement Messages.
Notes	Does not apply when sending Acknowledgement Messages.

3.4.14. RSC-SEN150 Sending Edge Node must check MSH-3 and MSH-4

RSC #	RSC-SEN150
RSC Name	Sending Edge Node must check MSH-3 and MSH-4
Requirement	*R120 Sending System must be able to receive Message Acknowledgement*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL validate that the values in MSH-3 and MSH-4 against those of the au-receivingapplication and au-receivingfacility fields respectively of the Endpoint that the Sending System will use to receive the Message Acknowledgements.
Notes	The au-receivingapplication is an optional field in the AU-FHIR Provider Directory Implementation Guide. Receivers may choose to publish au-receivingapplication in the AU-FHIR Provider Directory to facilitate application routing on the receiving end. The Sending Edge Node MUST honour what the Receiver has published / chosen to omit in the au-receivingapplication field. The MSH-3 element is defined in Section 2.1.9.3 of the Australian Diagnostics and Referral Messaging – Localisation of HL7 Version 2.4. The MSH-4 element is defined in Section 2.1.9.4 of the Australian Diagnostics and Referral Messaging – Localisation of HL7 Version 2.4. Failures in validating addressing details MAY be communicated using HL7 v2 ACK with AE code, or an alternative mechanism as agreed between the Sending Edge Node and the Sending System.

3.4.15. RSC-SEN160 Sending Edge Nodes – retry or Application Error Acknowledgement

RSC #	RSC-SEN160
RSC Name	Sending Edge Nodes – retry or Application Error Acknowledgement
Requirement	*R130 Delivery re-try*
Applies to Role	Sending Edge Nodes

Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL retry failed send invocations until invocation is successful. If the invocation fails, the Sending Edge Node SHALL communicate to the Sending System. This SHALL be done using either HL7 v2 ACK with AE code (as defined HL7 Table 0008 – Acknowledgement Code in Section 2.1.8.18.3 of Australian Diagnostics and Referral Messaging – Localisation of HL7 Version 2.4), or an alternative mechanism as agreed between the Sending Edge Node and the Sending System.
Notes	ATS-5822 Section 3.3.6 (a) p16, Section 5.4.1 (c) p23, Section 6.4.1 (c) p27

3.4.16. RSC-SEN170 Re-use same Invocation Identifier after invocation failure

RSC #	RSC-SEN170
RSC Name	Re-use same Invocation Identifier after invocation failure
Requirement	*R130 Delivery re-try*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	If an invocation is retried due to an invocation failure, the Sending Edge Node SHALL use the same Invocation Identifier.
Notes	ATS5822 Section 3.3.6 (b) p16

3.4.17. RSC-SEN180 No re-use of Invocation Identifier after success

RSC #	RSC-SEN180
RSC Name	No re-use of Invocation Identifier after success
Requirement	*R130 Delivery re-try*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL not re-use previously used Invocation Identifiers in a Sealed Message Delivery interface invocation if resending a message after a Transport Response is received for that invocation.

Notes	ATS-5822 Section 3.3.6 (d) p16 "Receipt of a Final Transport Response indicates that a previous invocation was successful".

3.4.18. RSC-SEN230 Received FTRs from Core Nodes

RSC #	RSC-SEN230
RSC Name	Received FTRs from Core Nodes
Requirement	*R160 Delivery must be reliable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL have a mechanism to receive both successful and error responses from their Core Node. Final Transport Responses SHOULD be used for these responses or an alternative mechanism MAY be used as agreed between the Sending Edge Node and the Core Node.
Notes	

3.4.19. RSC-SEN240 Escalate unrecognised Invocation Identifier

RSC #	RSC-SEN240
RSC Name	Escalate unrecognised Invocation Identifier
Requirement	*R160 Delivery must be reliable*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	When the Invocation Identifier associated with a Final Transport Response does not match any invocation made by the Sending Edge Node, the Sending Edge Node SHALL escalate the issue to a Responsible Person using an approved escalation mechanism as per RSC-G50.
Notes	ATS-5822 Section 3.4.4 p17 RSC-G50 Maintain system log

3.4.20. RSC-SEN250 Sealed Messages signed

RSC #	RSC-SEN250

RSC Name	Sealed Messages signed
Requirement	*R200 Sender Authenticated* *R220 Message integrity confirmed*
Applies to Role	Sending Edge Nodes
Optionality	MANDATORY
Solution Constraint	Sending Edge Nodes SHALL sign Sealed Messages in accordance with the ATS-5821 Standard with the Author Organisation's Private Key issued by an approved Certificate Authority (CA) – see Appendix B, recognising the need to update: • signatureMethod and digestMethod to a current minimum of RSA-SHA256 • encryption from RSA 1.5 to the currently recommended mandatory minimum AES-128 GCM
Notes	

3.5. Requirements and solution constraints: Core Nodes

3.5.1. RSC-CN10 Core Nodes implement Provider Directory

RSC #	RSC-CN10
RSC Name	Core Nodes implement Provider Directory
Requirement	*R10 Search supported*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL implement and advertise their Receiving Edge Nodes Endpoints in their Provider Directory.
Notes	

3.5.2. RSC-CN20 Core Node connectivity

RSC #	RSC-CN20
RSC Name	Core Node connectivity
Requirement	*R10 Search supported*
Applies to Role	Core Nodes

Optionality	MANDATORY
Solution Constraint	Core Node SHALL directly connect to all other Core Nodes in the NSMN.
Notes	

3.5.3. RSC-CN40 Identifier in certificate matches Endpoint identifier

RSC #	RSC-CN40
RSC Name	Identifier in certificate matches Endpoint identifier
Requirement	*R10 Search supported*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL validate that the identifier in the PKI certificate for Endpoints matches the identifier in the corresponding Endpoint data published in the Provider Directory. When the identifiers do not match, message transmission SHALL be terminated, and an appropriate error Final Transport Response SHALL BE generated.
Notes	Section 2.4 of the Secure Message Addressing Implementation Guide provides further guidance on conformance:

3.5.4. RSC-CN50 Use of Public Key Infrastructure for Provider Directory authentication

RSC #	RSC-CN50
RSC Name	Use of Public Key Infrastructure for Provider Directory Authentication
Requirement	*R20 Authorised searching only*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Authentication: When connecting over a public network to the Provider Directory, Sending System, Sending Edge Node or Receiving Edge Node, the Core Node SHALL authenticate the identity of the connecting entity using Public Key Infrastructure (PKI). Assert Identity: When connecting over a public network to the Provider Directory, Sending System, Sending Edge Node or Receiving Edge Node, the

	Sending Edge Node SHALL assert the identity of the organisation operating the system to the connecting system.
Notes	

3.5.5. RSC-CN80 Receive Messages from Sending Edge Nodes

RSC #	RSC-CN80
RSC Name	Receive Messages from Sending Edge Nodes
Requirement	*R110 Messages transmittable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL have a mechanism to receive Messages from their Sending Edge Nodes.
Notes	ATS-5822 Section 3.2 provides a mechanism for this purpose. However, other proprietary mechanisms MAY be used.

3.5.6. RSC-CN90 Core Node to Core Node Message exchange – implement Message Delivery interface

RSC #	RSC-CN90
RSC Name	Core Node to Core Node Message exchange - implement Message Delivery interface
Requirement	*R110 Messages transmittable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	The Core Node SHALL be able to exchange Sealed Messages with other Core Nodes in accordance with the ATS-5822 Standard. The Core Node SHALL implement a Sealed Message Delivery interface as specified in ATS-5822, Section 8.
Notes	

3.5.7. RSC-CN92 Core Node to Core Node Message exchange - invoke Message Delivery interface

RSC #	RSC-CN92

RSC Name	Core Node to Core Node Message exchange - invoke Message Delivery interface
Requirement	*R110 Messages transmittable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	The Core Node SHALL be able to exchange Sealed Messages with other Core Nodes in accordance with the ATS-5822 Standard. The Core Node SHALL have the ability to invoke each other Core Node's Sealed Message Delivery interface.
Notes	

3.5.8. RSC-CN94 Core Node to Core Node Message exchange – implement Transport Response Delivery interface

RSC #	RSC-CN94
RSC Name	Core Node to Core Node Message exchange – implement Transport Response Delivery Interface
Requirement	*R110 Messages transmittable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	The Core Node SHALL be able to exchange Secure Messages with other Core Nodes in accordance with the ATS-5822 Standard. The Core Node SHALL implement a Transport Response Delivery Interface as specified in ATS-5822, Section 11.
Notes	

3.5.9. RSC-CN96 Core Node to Core Node Message exchange – invoke Transport Response Delivery interface

RSC #	RSC-CN96
RSC Name	Core Node to Core Node Message exchange – invoke Transport Response Delivery interface
Requirement	*R110 Messages transmittable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	The Core Node SHALL be able to exchange Secure Messages with other Core Nodes in accordance with the ATS-5822 Standard. The Core Node SHALL have the ability to invoke each other Core Node's Transport Response Delivery interface.

Notes	

3.5.10. RSC-CN100 Transmit Message to Receiving Edge Nodes

RSC #	RSC-CN100
RSC Name	Transmit Message to Receiving Edge Nodes
Requirement	*R110 Messages transmittable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL have a mechanism to deliver Messages to their Receiving Edge Nodes.
Notes	ATS-5822 provides a mechanism for this purpose. However, other proprietary mechanisms MAY be used if agreed between Core Node and Receiving Node providers.

3.5.11. RSC-CN110 Core Nodes – retry or error transport response

RSC #	RSC-CN110
RSC Name	Core Nodes – retry or error transport response
Requirement	*R130 Delivery re-try*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL retry failed send invocations until invocation is successful. If the invocation fails, the Core Node SHALL send a Transport Response to the upstream entity (Sending Edge Node or previous Core Node) indicating the delivery was unsuccessful.
Notes	The Transport Response action is defined in ATS-5822 Section 2.8 p10.

3.5.12. RSC-CN120 No re-try after Message expiry

RSC #	RSC-CN120
RSC Name	No re-try after Message expiry
Requirement	*R150 Messages not transmitted after expiry*

Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL not retry delivery invocation after the expiry time nominated in the Sealed Message metadata has passed.
Notes	ATS-5822 Section 3.3.6 (a) p16 "The expiryTime is inserted in the metadata fields of the Sealed Message by the Sending Edge Node as specified in Section B2.3 of ATS-5822 (p56)".

3.5.13. RSC-CN130 FTR if Message expires

RSC #	RSC-CN130
RSC Name	FTR if Message expires
Requirement	*R160 Delivery must be reliable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL generate and deliver one of the following if a Message cannot be delivered by its expiry time: • When the Message is received from another Core Node, an Error Final Transport Response • When the Message is received from their Sending Edge Node, an Error Final Transport Response or an alternative notification as agreed between a Core Node and its Sending Edge Node.
Notes	

3.5.14. RSC-CN140 Deliver FTRs to Sending Edge Node

RSC #	RSC-CN140
RSC Name	Deliver FTRs to Sending Edge Node
Requirement	*R160 Delivery must be reliable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL have a mechanism to deliver Final Transport Responses, or alternative notifications as agreed between Sending Edge Node and Core Node, to the Sending Edge Nodes.

Notes	ATS-5822 Section 2.8.2 p10

3.5.15. RSC-CN150 Deliver FTRs to Core Nodes

RSC #	RSC-CN150
RSC Name	Deliver FTRs to Core Nodes
Requirement	*R160 Delivery must be reliable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL have the ability to construct and deliver Final Transport Responses to other Core Nodes in accordance with the ATS-5822 Standard.
Notes	ATS-5822 Section 2.8.2 p10

3.5.16. RSC-CN160 Receive FTRs from Core Nodes

RSC #	RSC-CN160
RSC Name	Receive FTRs from Core Nodes
Requirement	*R160 Delivery must be reliable*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL have a mechanism to receive Final Transport Responses from other Core Nodes in accordance with the ATS-5822 Standard.
Notes	ATS-5822 Section 2.8.2 p10

3.5.17. RSC-CN170 Receive FTRs from Receiving Edge Nodes

RSC #	RSC-CN170
RSC Name	Receive FTRs from Receiving Edge Nodes
Requirement	*R160 Delivery must be reliable*
Applies to Role	Core Nodes
Optionality	MANDATORY

Solution Constraint	Core Nodes SHALL have a mechanism to receive Final Transport Response in accordance with the ATS-5822 Standard, or alternative notifications as agreed between Core Node and Receiving Edge Node
Notes	ATS-5822 Section 2.8.2 p10

3.5.18. RSC-CN180 Detect duplicate Invocation Identifiers

RSC #	RSC-CN180
RSC Name	Detect duplicate Invocation Identifiers
Requirement	*R240 Duplicate Messages detected*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	A request with the same Invocation Identifier as a previous request that was successfully processed is considered a duplicate. The Core Node SHALL return a status of duplicate in the response for duplicates received before the expiry time in the original Message has passed. The Core Node SHOULD consider clock skew when testing the expiry time.
Notes	ATS-5822 Section 8.2.2.4.1 p3 "A request with the same Invocation Identifier as a previous request that was successfully processed is considered a duplicate. The service provider shall return a status of duplicate in the response for any duplicates received before the expiryTime in the original Message has passed. The service provider should consider clock skew when testing the expiryTime."

3.5.19. RSC-CN190 Cease duplicate detection after expiry

RSC #	RSC-CN190
RSC Name	Cease duplicate detection after expiry
Requirement	*R240 Duplicate Messages detected*
Applies to Role	Core Nodes
Optionality	RECOMMENDED
Solution Constraint	Core Nodes MAY cease duplicate detection on an Invocation Identifier after the expiry time nominated in the Sealed Message metadata has passed. They SHOULD allow for clock skew and transmission delay equivalent to the difference between the Sealed Message creation time and time of receipt.

Notes	ATS-5822 5.4.1 (g) p24, ATS-5822 6.4.1 (g) p28 "The Intended Recipient [Author Intermediary and Intended Recipient Intermediary] may cease duplicate detection on an Invocation Identifier after the expiryTime nominated in the Sealed Message metadata has passed. The Intended Recipient should allow for clock skew and transmission delay equivalent to the difference between the Message creation time and time of receipt."

3.5.20. RSC-CN200 Core Nodes SHALL not decrypt Sealed Messages

RSC #	RSC-CN200
RSC Name	Core Nodes SHALL not decrypt Sealed Messages
Requirement	*R310 No unauthorised access to Messages*
Applies to Role	Core Nodes
Optionality	MANDATORY
Solution Constraint	Core Nodes SHALL not decrypt Sealed Messages.
Notes	ATS-5822 Section 6.3.2 (b) p7 "The Intended Recipient Intermediary shall not decrypt any sealed payload. In other words, in the unlikely event of the Intended Recipient Intermediary having a copy of the Intended Recipient private key, this key SHALL not be used to decrypt any Messages or transport responses."

3.6. Requirements and solution constraints: Receiving Edge Nodes

3.6.1. RSC-REN10 Receive Sealed Messages from Core Node

RSC #	RSC-REN10
RSC Name	Receive Sealed Messages from Core Node
Requirement	*R110 Messages transmittable*
Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL have a mechanism to receive Sealed Messages from their Core Nodes.

Notes	ATS-5822 Section 6 provides a mechanism for this purpose, although other proprietary mechanisms can be used as agreed between Core Nodes and Receiving Edge Nodes.

3.6.2. RSC-REN20 Transmit Messages to Receiving System

RSC #	RSC-REN20
RSC Name	Transmit Messages to Receiving System
Requirement	*R110 Messages transmittable*
Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL have a mechanism to deliver Clinical Messages to their Receiving System.
Notes	**File Drop:** The exchange of standard HL7 V2 Payloads via a local file system is a common convention for the exchange of Messages between Edge Nodes and Sending or Receiving Systems.

3.6.3. RSC-REN30 Receiving Edge Nodes – retry or error transport response

RSC #	RSC-REN30
RSC Name	Receiving Edge Nodes – retry or error transport response
Requirement	*R130 Delivery re-try*
Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL retry failed send invocations until invocation is successful. If the invocation fails, then the system SHALL send a Transport Response to the upstream core node indicating the delivery was unsuccessful.
Notes	The Transport Response is defined in ATS-5822 Section 2.8 p10.

3.6.4. RSC-REN40 No re-try after Message expiry

RSC #	RSC-REN40
RSC Name	No re-try after Message expiry
Requirement	*R150 Messages not transmitted after expiry*

Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL NOT try or retry delivery invocation after the Message expiry time.
Notes	ATS-5822 Section 3.3.6 (a) p16 "The expiryTime is inserted in the Sealed Message by the Sending Edge Node as specified in Section B2.3 of ATS-5822 (p56)."

3.6.5. RSC-REN50 Generate FTR to Core Node if message expires

RSC #	RSC-REN50
RSC Name	Generate FTR to Core Node if message expires
Requirement	*R160 Delivery must be reliable*
Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL generate and deliver an Error Final Transport Response to their Core Node, or alternative notification as agreed between the Core Node and Receiving Edge Node, if a Message cannot be delivered by its expiry time.
Notes	ATS-5822 Section 9.2.2.4.2 (b) specifies a timeoutError fault response if the Message cannot be delivered by the expiryTime. Section 9.1.3 shows the schema for the timeout error.

3.6.6. RSC-REN60 Deliver FTRs to Core Node

RSC #	RSC-REN60
RSC Name	Deliver FTRs to Core Node
Requirement	*R160 Delivery must be reliable*
Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL have a mechanism to create and deliver Final Transport Responses, or alternative notifications as agreed between the Receiving Edge Node and Core Node, to their Core Node.
Notes	

3.6.7. RSC-REN70 Retry FTR delivery or escalate

RSC #	RSC-REN70
RSC Name	Retry FTR delivery or escalate
Requirement	*R160 Delivery must be reliable*
Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL either retry delivery of Final Transport Responses, or alternative notifications as agreed between Core Node and Receiving Edge Node, to their Core Node, or escalate the issue to a Responsible Person as per RSC-G50.
Notes	ATS-5822 Section 3.4.4 (c) p17 RSC-G50

3.6.8. RSC-REN80 Check digital signature on received Sealed Messages

RSC #	RSC-REN80
RSC Name	Check digital signature on received Sealed Messages
Requirement	*R200 Sender Authenticated* *R220 Message integrity confirmed*
Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	Receiving Edge Nodes SHALL verify that the signature on an incoming Sealed Message was made with the nominated signing Certificate and SHALL validate the authenticity of the signing Certificate. This validation is to ensure that the identity information contained in the certificate matches the identity information of the Sender contained in the metadata of the Sealed Message or identifies an authorised agent of the Sender.
Notes	ATS-5822 Section 4.3.7 (a) p20

3.6.9. RSC-REN110 Detect duplicate Invocation Identifiers

RSC #	RSC-REN110
RSC Name	Detect duplicate Invocation Identifiers
Requirement	*R240 Duplicate Messages detected*

Applies to Role	Receiving Edge Nodes
Optionality	MANDATORY
Solution Constraint	A request with the same Invocation Identifier as a previous request that was successfully processed is considered a duplicate. a) The Receiving Edge Node SHALL return a status of "duplicate" in the response for any duplicates received before the expiry time nominated in the metadata of the original Sealed Message has passed. b) The Receiving Edge Node SHOULD consider clock skew when testing the expiry time.
Notes	ATS-5822 Section 8.2.2.4.1 (c) p34

3.6.10. RSC-REN120 Cease duplicate detection after expiry

RSC #	RSC-REN120
RSC Name	Cease duplicate detection after expiry
Requirement	*R240 Duplicate Messages detected*
Applies to Role	Receiving Edge Nodes
Optionality	RECOMMENDED
Solution Constraint	Receiving Edge Nodes MAY cease duplicate detection on an Invocation Identifier after the expiry time nominated in the metadata of the Sealed Message has passed. They SHOULD allow for clock skew and transmission delay equivalent to the difference between the Sealed Message creation time and time of receipt.
Notes	ATS-5822 Section 4.3.3 (b) p19, Section 5.4.1 (g) p28

3.7. Requirements and solution constraints: Receiving Systems

3.7.1. RSC-RS10 Receive Messages from Receiving Edge Node

RSC #	RSC-RS10
RSC Name	Receive Messages from Receiving Edge Node
Requirement	*R110 Messages transmittable*
Applies to Role	Receiving Systems
Optionality	MANDATORY

Solution Constraint	Receiving Systems SHALL have a mechanism to receive Messages from their Receiving Edge Node.
Notes	ATS-5822 Section 6 provides a mechanism for this purpose, although other proprietary mechanisms MAY be used as agreed between Receiving System and Receiving Edge Node. At this stage of processing, these are not Sealed Messages but decrypted clear/text Messages e.g. HL7 messages.

3.7.2. RSC-RS20 Generate and send Application Acknowledgement

RSC #	RSC-RS20
RSC Name	Generate and send Application Acknowledgement
Requirement	*R190 Receiving System must be able to generate and send Message Acknowledgement*
Applies to Role	Receiving Systems
Optionality	MANDATORY
Solution Constraint	Receiving Systems SHALL generate and send the appropriate Application Acknowledgement on receipt of a Clinical Message as per the HL7 Australia Acknowledgement Specification – see Appendix A. Details of Application Acknowledgement codes are defined in MSA-1.
Notes	

3.7.3. RSC-RS21 Generate and send User Read Acknowledgement

RSC #	RSC-RS21
RSC Name	Generate and send User Read Acknowledgement
Requirement	*R190 Receiving System must be able to generate and send Message Acknowledgement*
Applies to Role	Receiving Systems
Optionality	RECOMMENDED
Solution Constraint	Receiving Systems MAY generate a User Read Acknowledgement
Notes	User Read Acknowledgements serve the purpose of notifying the Author that a specific Intended Recipient has viewed the Clinical Message, and confirming they have read the content. Receiving Systems MAY generate and send a User Read Acknowledgement to a received Clinical Message (as per Section 8.4 of HL7 Australia Acknowledgement Specification) – see Appendix A.

3.7.4. RSC-RS30 Must receive standard message formats

RSC #	RSC-RS30
RSC Name	SHALL receive standard message formats
Requirement	*R170 Received Messages are able to be*
Applies to Role	Receiving Systems
Optionality	MANDATORY
Solution Constraint	Receiving Systems SHALL be able to accept and successfully process Message in standard formats – see Appendix A. For every Message Category (set out in Table 1) the Receiving System accepts, it MUST accept all Clinical Message formats in that category as specified in **Principle #2**.
Notes	

3.7.5. RSC-RS40 May receive non-standard formats

RSC #	RSC-RS40
RSC Name	May receive non-standard formats
Requirement	*R170 Received Messages are able to be processed*
Applies to Role	Receiving Systems
Optionality	MAY
Solution Constraint	Receiving Systems MAY be able to accept and successfully process non-standard Clinical Message formats.
Notes	Standard formats are listed in Appendix A

3.7.6. RSC-RS41 Received messages are protected with access controls

RSC #	RSC-RS41
RSC Name	Received messages are protected with access controls
Requirement	*R310 No unauthorised access to Messages*
Applies to Role	Receiving Systems
Optionality	MANDATORY

Solution Constraint	Receiving Systems SHALL ensure Clinical Messages can only be accessed by authorised user accounts but are not prescribed a method for doing so.
Notes	

3.7.7. RSC-RS50 Received Messages accurately presented for action

RSC #	RSC-RS50
RSC Name	Received Messages accurately presented for action
Requirement	*R180 Received Messages accurately presented for action*
Applies to Role	Receiving Systems
Optionality	MANDATORY
Solution Constraint	Receiving Systems SHALL be able to render complex Clinical Messages.
Notes	ATS-5822 Section 4.3.6 p20 Examples of complex messages

3.7.8. RSC-RS51 Duplicate Messages accurately identified

RSC #	RSC-RS51
RSC Name	Duplicate Messages accurately identified
Requirement	*R240 Duplicate Messages detected*
Applies to Role	Receiving Systems
Optionality	MANDATORY
Solution Constraint	Receiving Systems SHALL meet this requirement by demonstrating identification of duplicate Clinical Messages. The HL7 segments MSH-4 + MSH-10 SHALL be used for duplicate detection. The Clinical Message SHALL be processed and acknowledged.
Notes	Duplicates are identified as per Unique IDs in header. Duplicates are not considered to be errors for the purpose of generating and sending an Acknowledgement.

3.7.9. RSC-RS60 Check signature on received CDA Documents

RSC #	RSC-RS60
RSC Name	Check signature on received CDA Documents
Requirement	*R200 Sender Authenticated* *R220 Message integrity confirmed*
Applies to Role	Receiving Systems
Optionality	MANDATORY
Solution Constraint	Where a Payload contains a CDA Document, the Receiving System SHALL check the digital signature associated with the CDA Document, including: a) verifying that the signature on the incoming CDA Document was made with the nominated signing Certificate, and b) validating the authenticity of the signing Certificate. When the checks fail, the Message SHALL be retained for review and action by the Responsible Person (refer RSC-G50 Escalation Pathway.)
Notes	

3.7.10. RSC-RS90 Intended Recipient able to reconcile messages

RSC #	RSC-RS90
RSC Name	Intended Recipient able to reconcile messages
Requirement	*R260 Intended Recipients able to reconcile Messages*
Applies to Role	Receiving Systems
Optionality	MANDATORY
Solution Constraint	None. Receiving Systems SHALL meet requirement R260 but are not prescribed a method for doing so.
Notes	

3.8. Requirements and solution constraints: Provider Directory

3.8.1. RSC-PD10 Use of Public Key Infrastructure for authentication

RSC #	RSC-PD10
RSC Name	Use of PKI for authentication

Requirement	*R20 Authorised searching only*
Applies to Role	Source Provider Directories
Optionality	MANDATORY
Solution Constraint	Authentication: When connecting to the Provider Directory over a public network, the connecting entity SHALL authenticate the identity of the Provider Directory using Public Key Infrastructure (PKI). Assert Identity: When connecting to the Provider Directory over a public network, the calling entity SHALL assert the identity of the organisation operating the entity to the Provider Directory.
Notes	See Appendix B for Approved Certificate Authorities. Other authentication and authorization protocols can be used if both the calling entity and Provider Directory agree

3.8.2. RSC-PD20 Provider Directories contain Receiving Edge Nodes

RSC #	RSC-SPD20
RSC Name	Provider Directories contain Receiving Edge Nodes
Requirement	*R10 Search supported*
Applies to Role	Provider Directories
Optionality	MANDATORY
Solution Constraint	Provider Directory SHALL support upload and persistence of Receiving Edge Node identifying information to enable Authors to identify Intended Recipients.
Notes	

3.8.3. RSC-PD30 Provider Directories source and federate results

RSC #	RSC-FPD20
RSC Name	Provider Directories source and federate results
Requirement	*R10 Search supported*
Applies to Role	Provider Directories
Optionality	MANDATORY

Solution Constraint	Upon request, Provider Directories SHALL be able to securely source and federate directory information about Edge Nodes contained in multiple NSMN Provider Directories into a uniform data structure as set out in the profiles section of the Australian Provider Directory Implementation Guide.
Notes	Provider Directories must support federation on request in order to remain current. Federation of Directory Information mirrors direct connectivity between Core Nodes (one hop federation only).

3.8.4. RSC-PD40 Provider Directories support search

RSC #	RSC-PD40
RSC Name	Provider Directories support search
Requirement	*R10 Search supported*
Applies to Role	Provider Directories
Optionality	MANDATORY
Solution Constraint	Provider Directory SHALL support search capability to enable Authors to identify potential Intended Recipients. The Provider Directory SHALL support all search capabilities that are specified as "MUST support" in the profiles section of the Australian Provider Directory Implementation Guide.
Notes	

3.8.5. RSC-PD50 Provider Directory support paging result sets

RSC #	RSC-PD50
RSC Name	Provider Directory support paging result sets
Requirement	*R10 Search supported*
Applies to Role	Provider Directory
Optionality	MANDATORY
Solution Constraint	Source Provider Directory SHALL support paging of result sets.
Notes	As per requirement FED04 of Federation of Directory Services

3.9. Requirements and solution constraints: General

3.9.1. RSC-G10 All Endpoints to use Web Services Base Profile

RSC #	RSC-G10
RSC Name	All Endpoints to use Web Services Base Profile
Requirement	*R300 Messages protected in transit*
Applies to Role	All Systems
Optionality	MANDATORY
Solution Constraint	All Endpoints SHALL conform to the Web Services Base Profile from the ATS-5820 E-Health Web Services Profiles for all Web services invocations.
Notes	ATS-5822 Section 2.2.1 p8

3.9.2. RSC-G20 Endpoints to use TLS-1.2 or greater

RSC #	RSC-G20
RSC Name	Endpoints to use TLS-1.2 or greater
Requirement	*R300 Messages protected in transit*
Applies to Role	All Systems
Optionality	MANDATORY
Solution Constraint	All Endpoints SHALL use TLS-1.2 as the minimum version. Sending and Receiving systems MAY agree to implement a higher version of TLS. Especially weak encryption algorithms in TLS 1.2 are designated as NULL, RC2, RC4, DES, IDEA, and TDES/3DES; cipher suites using these algorithms MUST NOT be used. TLS 1.3 removes these cipher suites, but implementations that support both TLS 1.3 and TLS 1.2 MUST be checked for obsolete cipher suites.
Notes	ATS-5822 Section 2.2.1 (b) p8 ATS-5820 Section 8.2.1 p34 references TLS 1.0. This has been superceded by TLS 1.2 as the minimum. Entities SHALL NOT establish connections using TLS 1.0.

3.9.3. RSC-G30 Endpoints to validate Certificates of invokers

RSC #	RSC-G30
RSC Name	Endpoints to validate Certificates of invokers
Requirement	*R300 Messages protected in transit*
Applies to Role	All Systems
Optionality	MANDATORY
Solution Constraint	All Endpoints SHALL validate the transport Certificate(s) of any invoker of its service interfaces, i.e. the Certificate(s) used to establish a TLS connection. This validation SHOULD ensure that the identity information contained in the Certificate adequately identifies the source of the invocation.
Notes	ATS-5822 Section 3.4.2 (b) p16, Section 4.3.7 (b) p20, Section 5.3.2 (b) p23, Section 6.3.2 (b) p27.

3.9.4. RSC-G40 TLS 1.2 or greater used over all public networks

RSC #	RSC-G40
RSC Name	TLS 1.2 or greater used over all public networks
Requirement	*R310 No unauthorised access to Messages*
Applies to Role	All Systems
Optionality	MANDATORY
Solution Constraint	All solutions SHALL ensure Messages are not transmitted across any public network without a minimum of TLS 1.2 or greater as agreed between sending and receiving entities. Especially weak encryption algorithms in TLS 1.2 are designated as NULL, RC2, RC4, DES, IDEA, and TDES/3DES; cipher suites using these algorithms MUST NOT be used. TLS 1.3 removes these cipher suites, but implementations that support both TLS 1.3 and TLS 1.2 MUST be checked for obsolete cipher suites.
Notes	ATS-5820 Section 8.2.1 p34 references TLS 1.0. This has been superseded by TLS 1.2 as the minimum. Entities SHALL NOT establish connections using TLS 1.0.

3.9.5. RSC-G50 Escalation Pathway

RSC #	RSC-G50
RSC Name	Escalation to a Responsible Person in exception event
Requirement	*R310 No unauthorised access to Messages*
Applies to Role	Sending System, Sending Edge Node, Core Node, Receiving Edge Node, Receiving System
Optionality	MANDATORY
Solution Constraint	The solution SHALL have a mechanism to escalate an important event that occurs at any Node for the applicable roles to a Responsible Person.
Notes	

3.9.6. RSC-G60 Maintain system log

RSC #	RSC-G60
RSC Name	Maintain system log
Requirement	*R160 Delivery must be reliable*
Applies to Role	Sending System, Sending Edge Node, Core Node, Receiving Edge Node, Receiving System
Optionality	MANDATORY
Solution Constraint	The system SHALL maintain a log for incident resolution and audit purposes.
Notes	

4. Appendix A – Standard Message formats

Interoperable secure messaging requires that Sending Systems are able to generate Messages in formats that Receiving Systems can successfully process. To enable this, the following two principles must be satisfied:

Principle #1 – Sending Systems must generate one or more standard Clinical Message formats per supported category

For each Message Category (see Table 1) a Sending System supports, it must be able to generate outbound Clinical Messages in at least one of the standard formats listed in table below.

For example, if a Sending System is used to generate referrals, the Sending System must be able to generate either REF-I12 Clinical Messages, MDM-T02 Clinical Messages, or both. The Sending System may, if it chooses, support additional non-standard message formats only for new message categories.

For each standard Clinical Message it supports, the Sending System must be able to receive and successfully process the associated Acknowledgement Messages. For example, if a Sending System generates and sends REF-I12 messages, it must also be able to receive RRI-I12 Accept Acknowledgement Messages (in addition to the Application Acknowledgement Messages), as per the HL7 Acknowledgement specification).

Principle #2 – Receiving Systems must be able to receive *all* standard Clinical Message formats per supported category.

For each Message Category a Sending System supports, it must be able to receive inbound Clinical Messages in all standard formats listed below.

For example, if a Receiving System supports inbound referrals, it must be able to receive and process referrals in both REF-I12 and MDM-T02 format. The Receiving System must also be capable of generating and sending the associated Accept Acknowledgement Messages, RRI-I12 and ACK-T02 (in addition to Application Acknowledgement Messages, as per the HL7 Acknowledgement specification).

The Receiving System may, if it chooses, support additional non-standard message formats only for new message categories.

NB: All systems that receive inbound Clinical Messages must be able to generate and send Application Acknowledgement Messages, as per the HL7 Acknowledgement specification, in addition to the Acknowledgement Messages listed in the table below.

Message Category	Clinical Message format	Acknowledgement Message format
Referrals	HL7 v2.4 REF^I12-L1	RRI^I12
	Agency Service Referral CDA package wrapped with HL7 v2.3.1 MDM^T02	ACK^T02
Discharge summaries	HL7 v2.4 REF^I12-L1	RRI^I12
	Agency Discharge Summary CDA package wrapped with HL7 v2.3.1 MDM^T02	ACK^T02
Specialist letters	HL7 v2.4 REF^I12-L1	RRI^I12
	Agency Specialist Letter CDA package wrapped with HL7 v2.3.1 MDM^T02	ACK^T02
	HL7 v2.4 ORU^R01	ACK^R01
Observation orders	HL7 v2.4 ORM^O01	ACK^O01
Observation results	HL7 v2.4 ORU^R01	ACK^R01

Table 1 Message Categories and Clinical Formats

5. Appendix B – Approved Certificate Authorities (CA)

The NSMN requires that X509v3 digital certificates issued by an approved Certificate Authority are used for the following purposes:

1. creating (and checking) digital signatures of CDA documents[2]
2. creating (and checking) digital signatures of Sealed Messages
3. encryption and decryption of Sealed Messages

The following table lists the currently approved list of Certificate Authorities:

Acronym	Full Name	More information
NASH	National Authentication Service for Health	https://www.servicesaustralia.gov.au/organisations/health-professionals/services/medicare/national-authentication-service-health

[2] Only NASH based certificates can sign CDA documents

6. Glossary

6.1. Information Systems / Technical Roles

Authorised User

- A user of a Sending or Receiving System that has been authorised to conduct searches using Provider Directories

Core Node

- A Core Node is responsible for exchanging Sealed Messages securely with other Core Nodes in the NSMN and providing message sending and receiving services for their connected Edge Nodes. A Core Node is also responsible for maintaining and exposing a Provider Directory containing address information for its Receiving Edge Nodes.

Endpoint

- A service interface exposed by a Receiving Edge Node where a Sealed Message can be delivered.

Internal Information System

- A Sending System, Receiving System, or Relay System

Local Address Book

- Definition TBC

Provider Directory

- A Provider Directory is an electronic directory of Healthcare Providers and associated entities that conforms to the Australian Provider Directory Implementation Guide (PD 2) specification.

Receiving Edge Node

- A Receiving Edge Node is the interface between a Core Node and the Internal Information Systems used by the Receiver. A Receiving Edge Node is a delivery point in the NSMN with a logical address where a Sealed Message containing a Clinical Message or Acknowledgement Message can be received. After receiving a Sealed Message from a Core Node, Receiving Edge Nodes decrypt them, check their digital signature and transmit their Payload to the Receiving System, directly or via Relay System(s). A Receiving Edge Node is represented in a Provider Directory by one or more Endpoint entries.

Receiving System

- A Receiving System is an information system used by the Receiver. It is responsible for processing Messages received via the NSMN and making their content available to Receivers so that related business processes can be executed.

Relay System

- A Relay System is an intermediate system between a Sending System and a Sending Edge Node, or a Receiving System and a Receiving Edge Node. The Relay System acts as an intermediary, relaying or forwarding Messages between the systems.

Sending Edge Node

- A Sending Edge Node is the interface between the Internal Information Systems used by the Sender and a Core Node. The Sending Edge Node receives Payloads to transmit (Clinical Messages or Acknowledgement Messages) from a Sending System or Relay System. A Sending Edge Node is responsible for signing, encrypting and transmitting the Payload, inside a Sealed Message, to a Core Node. A Sending Edge Node is also the delivery point in the NSMN with a logical address where a Sealed Message containing a Final Transport Response can be received.

Sending System

- A Sending System is an information system used by the Sender for the creation, management and release of Messages to be transmitted via the NSMN.

6.2. Parties

Administrator

- An administrator, such as a GP Practice Manager, may act on behalf of the Author (e.g. a GP) to facilitate the transmission of the clinical message.

Author

- An Author is a Practitioner or device that initiates the send of a Clinical Message or Acknowledgement Message via the NSMN, determines the Receivers, and authorises the release of the contained information for transmission.

Client

- A client is a Sending System or Receiving system as per roles defined in the NSMN Blueprint

Consumer

- A Consumer is the subject-of-care in the Clinical Message being transmitted or an authorised representative of the subject-of-care. Consumers are often referred to as patients.

Healthcare Service

- A Healthcare Service is a service whose Practitioner Roles deliver healthcare-related services to Consumers at a location. The formal data definition for Healthcare Service can be found here.

Intended Recipient

- A Intended Recipient is the Practitioner Role or Healthcare Provider who the Author intends as the recipient of their transmitted Clinical Message or Acknowledgement Message.

Organisation

- An Organisation is the legal entity operating a Healthcare Service. Organisation is defined in the Australian Provider Directory Implementation Guide (PD 2) specification.

Practitioner

- A Practitioner is a person who, when acting in a Practitioner Role, is directly or indirectly involved in the provisioning of healthcare-related services to Consumers. The formal data definition for Practitioner can be found here.

Practitioner Role

- A Practitioner Role is a Practitioner who, acting on behalf of a Healthcare Service, delivers healthcare-related services to Consumers at a location. A single Practitioner may act in multiple Practitioner Roles. The formal data definition for Practitioner Role can be found here.

Receiver

- A Receiver is the Organisation that operates the Internal Information Systems that deliver messages to the Intended Recipient.

Responsible Person

- An administrative person that has responsibility for managing and resolving clinical message issues as they relate to information system or technical role in the NSMN.

Sender

- A Sender is the Organisation that operates the Internal Information Systems that an Author uses to send a Message.

6.3.Messaging

Accept Acknowledgment Message (aka Accept Acknowledgement)

- An Accept Acknowledgement Message is a Payload sent by the Receiving System to the Sending System indicating storage status of a received Clinical Message. Accept Acknowledgement Messages are to be used as per the HL7 v2.4 specification.

Acknowledgment Message (aka Acknowledgement)

- Acknowledgement Message and Acknowledgement are general terms for Accept Acknowledgement Messages and Application Acknowledgement Messages.

Application Acknowledgement Messages (aka Application Acknowledgement)

- Application Acknowledgements are a Payload sent by the Receiving System to the Sending System indicating the status of a received Clinical Message. The format of an Application Acknowledgement Message is specific to the Clinical Message being acknowledged (e.g. RRI-I12 is the format of an Application Acknowledgement Message for a received REF-I12 Clinical Message. Application Acknowledgement Messages are to be used as per the HL7 v2.4 specification).

CDA Document

- Clinical documents based on Agency CDA document package, including e-Referral, Discharge Summary, Event Summary, Shared Health Summary, and Specialist Letter.

Clinical Message

- A Clinical Message is a HL7 Payload that a Sender transmits to a Receiver to communicate clinical information and/or request a service. A referral sent from a GP to a specialist, or a discharge summary sent from a hospital to a GP, are both examples of Clinical Messages.

Final Transport Response (FTR)

- A Final Transport Response is a transport-layer message generated by a Receiving Edge Node or Core Node for transmission back to a Sending Edge Node indicating the success or failure of the message delivery process. Final Transport Responses include both Success and Error messages, as per ATS-5822 section 2.8.3a.

Invocation Identifier and Response Identifier

- Invocation and response identifiers are used to support the end-to-end messaging process, pairing a particular message delivery with its matching transport responses. Invocation and Response identifiers are either—
    - a UUID encoded as a URN according to [RFC4122]; or
    - a URL based on a domain name registered by the creating endpoint, and an identifier that is unique at the creating endpoint.

Message

- Message is a general term for Clinical Messages and Acknowledgement Messages. Each Message is transmitted as a Payload of a Sealed Message.

Payload

- A general term for the content being transmitted inside a Sealed Message.

Public Key Infrastructure

- Set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public-keys.

Sealed Message

- Sealed Message is the XML message format defined in ATS-5822 specification, Appendix B2.3. The Sealed Message wraps the Payload being transmitted.

Secure Message Delivery

- Deferred: where the messaging process is one-way and any application or human response is a separate messaging interaction. End-to-end delivery confirmation is provided through a Transport Response mechanism.

- Immediate: where the messaging process is two-way and an application response is returned immediately in a single interaction.

Transport Response (TR)

- ATS5822 allows endpoints receiving a message via the Sealed Message Delivery operation to send Transport Responses back along the delivery route to indicate delivery status. Intermediate responses are optional to create or retransmit. There is a distinguished Final Transport Response (FTR) that indicates either successful delivery or an unrecoverable error.

User Read Acknowledgment Message

- User read acknowledgements serve the purpose of notifying the sender that a specific recipient has viewed the message and confirmed they have read the content. 8 Acknowledgement - HL7AUSD-STD-OO-ADRM-2021.1 - HL7 Australia

6.4. Indicative Requirement Levels

Indicative Requirement levels are set as per RFC2119 – Key words for use in RFCs to Indicate Requirement Levels:

MUST -This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT – This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

SHOULD – This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT – This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY – This word, or the adjective "OPTIONAL," mean that an item is truly discretionary.

FUTURE – This word means that objectives are provided as guidance or expectation and may or may not be accurate.

SEPARATION – This word means the prevention of reach-ability to designated resources.

6.5. Technical References Required By This Specification

The technical standards and specifications set out in the following sub-sections include content that SHALL be adopted.

6.5.1. Message Transport

Standards and guides provide the technical specifications required by this IS for the creation, transport and delivery of Sealed Messages which contain Messages as Payload.

Australian Standard ATS-5822 [ATS 5822-2010] Australian Technical Specification for E-Health Secure Message Delivery defines the control and routing information required to transmit a message to an intended recipient in a safe and secure manner regardless of the Payload. Although this standard is marketed as having been superseded by AS 5552-2013, ATS-5822 is to be adopted. ATS-5822 references the other standards listed below:

- [ATS 5821-2010] E-health XML secure payload profiles defines the mechanisms for representing signed and encrypted XML data to achieve authentication, integrity, confidentiality and non-repudiation of messages.
- [ATS 5820-2010] E-health web services profiles defines a base set of SOAP Web services to ensure interoperability and profiles for securing the Web services transport.
- [TR 5823-2010] Endpoint location service describes the technical architecture for a service to obtain the information to locate and invoke Web services instances.

6.5.2. Message Format and Delivery

The Secure Messaging – Addressing Implementation Guide v1.1 provides implementation guidance clarity on how identifiers held in Provider Directories and secure message addressing interact to support the delivery and receipt of Clinical Messages, It is very relevant to both developers of clinical information systems and secure messaging systems.

The HL7 Australia Standard Document [HL7AUSD-STD-OO-ADRM-2021.1] Australian Diagnostics and Referral Messaging – Localisation of HL7 Version 2.4 provides guidance for the formatting and delivery of Messages. Particular aspects of this document important to the delivery of Messages include:

- Sub-section 2.1.9 MSH – message header segment defines amongst others the source and destination of the Message. Sub-sections 2.1.9.3 MSH-3 Sending application and 2.1.9.4 MSH-4 Sending facility describe how to representation the Sending Application in a Message.
- Sub-section 2.1.9.6 MSH-6 Receiving facility identifies a unique Receiving Application from multiple identical instances of the same application.
- Sub-section 2.1.9.10 MSH-10 Message control ID uniquely identifies a Clinical Message.
- Section 8 Acknowledgements provides an overview of the acknowledgement process and specifies the use of HL7 enhanced mode for Clinical Message acknowledgement, including a requirement to implement both Accept and Application Acknowledgements as set out in sub-section 8.3 Accept vs Application Acknowledgements.
- The format of the Acknowledgement Message is set out in sub-section 2.1.8 MSA message acknowledgment segment. In particular, sub-section 2.1.8.1 MSA-1 Acknowledgment Codes specifies the valid acknowledgement codes.
- The format of timestamps used in HL7 messages is set out in sub-section 3.26 TS timestamp.
- The size limit for Messages is defined by the HL7au Identifier 000019 as set out in Appendix 5 Conformance Statements (Normative).

6.5.3. Australian Provider Directory Implementation

The Australian Provider Directory Implementation Guide sets out the capability requirements for implementing the provider directory services required by this IS, in particular the following sections:

- Section Profiles Defined lists the profiles which must be supported for searching the provider directory.
- Sub-section Profiles Defined - Secure Messaging Endpoint describes the content of a secure message Endpoint (definition) to which secure messages are delivered.
- Section Federation of Directory Services states the requirements for federation of directories.
- The Australian Secure Message Service Interfaces defines the codes for service interface types including that for secure message delivery (deferred mode) required by this specification.
- The Australian Endpoint Payload Types defines the code set for each of the standard message formats set out in Appendix A – Standard Message formats. These values are

used in the Australian Secure Messaging Endpoint Directory Entry Endpoint.payloadType.

6.5.4. Clinical Document Architecture Formatting

The [NEHTA-1229:2011] Clinical Documents - CDA Package v1.0 is a clinical package profile which describes the three logical models together with their serialisation. This interoperability specification requires that for a Clinical Message which is a CDA Document, the latter must be signed by the Sending System. Section 4 of the package provides a specification for the signature.

The Department of Health and Aged Care - Formatting Pathology Reports provides recommendations for the style and layout of text within pathology reports.

The [HL7AUSD-STD-OO-ADRM-2021.1] Australian Diagnostics and Referral Messaging - Localisation of HL7 Version 2.4 - 4 Observation - 4.11 SPIA Rendering of numeric results,ranges,units,previous results and flagging provides guidelines for rendering the stated components within the body of pathology reports.

6.5.5. IETF Standards

The [IETF RFC4122] A universally Unique Identifier (UUID) URN Namespace specifies a standard for generating a universally unique identifiers (also known as Globally Unique Identifiers GUIDs). Within the scope of this specification, these are required for creating Invocation Identifiers.